Cahiers de la recherche sur les droits fondamentaux

17 | 2019
La motivation des actes administratifs. Le droit français à la lumière du droit administratif comparé

Chronique de jurisprudence des droits numériques 2017-2018

Manon Decaux, Léa Duval, Alexandre Labbay, Yann Paquier et Morgan Pénitot

Édition électronique
URL : http://journals.openedition.org/crdf/3870
DOI : 10.4000/crdf.3870
ISSN : 2264-1246

Éditeur
Presses universitaires de Caen

Édition imprimée
Date de publication : 31 décembre 2019
Pagination : 217-132
ISBN : 978-2-84133-960-0
ISSN : 1634-8842

Référence électronique
Manon Decaux, Léa Duval, Alexandre Labbay, Yann Paquier et Morgan Pénitot, « Chronique de jurisprudence des droits numériques 2017-2018 », *Cahiers de la recherche sur les droits fondamentaux* [En ligne], 17 | 2019, mis en ligne le 06 février 2021, consulté le 06 février 2021. URL : http://journals.openedition.org/crdf/3870 ; DOI : https://doi.org/10.4000/crdf.3870

Chronique de jurisprudence des droits numériques 2017-2018

Manon DECAUX

Doctorante en droit public à l'université de Caen Normandie

Centre de recherche sur les droits fondamentaux et les évolutions du droit (CRDFED, EA 2132)

Léa DUVAL

Doctorante en droit public à l'université de Caen Normandie

Centre de recherche sur les droits fondamentaux et les évolutions du droit (CRDFED, EA 2132)

Alexandre LABBAY

Doctorant en droit public à l'université de Caen Normandie

Centre de recherche sur les droits fondamentaux et les évolutions du droit (CRDFED, EA 2132)

Yann PAQUIER

Doctorant en droit public à l'université de Caen Normandie

Centre de recherche sur les droits fondamentaux et les évolutions du droit (CRDFED, EA 2132)

Morgan PÉNITOT

Doctorant en droit public à l'université de Caen Normandie

Centre de recherche sur les droits fondamentaux et les évolutions du droit (CRDFED, EA 2132)

Cette deuxième édition de la chronique des droits numériques retrace une actualité relativement riche. Priorité a donc été donnée à l'étude de l'immixtion de la puissance publique dans la régulation du cyberespace.

Les conséquences de cette immixtion sur les libertés du fait d'une législation de plus en plus répressive attirent notre attention (I). Dans le contexte particulier de la lutte contre le terrorisme, les autorités administratives se sont dotées d'un arsenal juridique de saisie, de l'exploitation et de la conservation des données (A). La pénalisation du refus de remettre aux autorités judiciaires la clé de déchiffrement d'un moyen de cryptologie mérite également d'être étudiée (B). L'Internet, notamment par le truchement des réseaux sociaux, est quant à lui devenu un enjeu stratégique de l'État dans la lutte contre la manipulation de l'information, particulièrement en période électorale (C).

Quant au second champ d'étude de cette chronique, il est consacré aux relations entre l'administration et les administrés (II). L'*open data* par défaut, grand principe de la loi pour une République numérique (LRN)[1], semble relativement inégal dans son application, voire amoindri (A). Les actions de groupe en réparation des préjudices liés aux données à caractère personnel constituent également un enjeu important, y compris dans leur ouverture à l'encontre des pouvoirs publics (B). Enfin, les traitements algorithmiques sont de plus en plus utilisés dans le cadre de l'action administrative et soulèvent des questionnements relatifs à leur transparence (C).

I. Libertés et répressions

A. Le régime de la saisie, de l'exploitation et de la conservation des données dans le cadre de la lutte contre le terrorisme

L'utilisation croissante des nouvelles technologies à des fins terroristes a nécessité de doter les autorités administratives de techniques d'enquêtes et d'investigations numériques, notamment dans le cadre des perquisitions administratives durant la période où l'état d'urgence était instauré. Parmi ces mesures, il a notamment été octroyé aux autorités la possibilité de procéder à la saisie et l'exploitation de données informatiques. Nous verrons comment d'exceptionnel (1) ce régime a été intégré dans le droit commun (3) après avoir connu entre-temps une refonte plus stricte sous le regard du Conseil constitutionnel (2).

1. Le régime de la saisie et de l'exploitation de données : une innovation précipitée issue de l'état d'urgence

Innovation issue de la première loi de prorogation de l'état d'urgence du 20 novembre 2015[2], le régime de l'exploitation des données est inscrit à l'article 11, I de la loi nº 55-385 qui concerne le régime des perquisitions administratives. Ce dernier permet aux autorités administratives désignées à l'article 8 de la même loi d'ordonner des perquisitions en un lieu lorsqu'il existe des raisons

1. Loi nº 2016-1321 du 7 octobre 2016 pour une République numérique, *Journal officiel de la République française*, nº 235, 8 octobre 2016, texte nº 1.
2. Loi nº 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi nº 55-385 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions, *Journal officiel de la République française*, nº 270, 21 novembre 2015, p. 21665, texte nº 1.

de penser que ce lieu est fréquenté par une personne dont le comportement constitue une menace pour la sécurité et l'ordre publics[3]. Dans ce cadre, les autorités administratives ont la possibilité d'accéder aux données informatiques découvertes et stockées sur des supports se trouvant sur les lieux de la perquisition[4]. Ce même dispositif octroie aux autorités la possibilité de copier ces données[5].

Dans sa décision du 19 février 2016, le Conseil constitutionnel est amené, à l'occasion d'une question prioritaire de constitutionnalité (QPC), à se prononcer sur ces dispositions[6]. Assimilant la copie des données à une saisie[7], le Conseil constitutionnel a estimé que

> […] ni cette saisie ni l'exploitation des données ainsi collectées ne sont autorisées par un juge, y compris lorsque l'occupant du lieu perquisitionné ou le propriétaire des données s'y oppose et alors même qu'aucune infraction n'est constatée […][8].

Il remarque également que la mesure semble disproportionnée dans le sens où

> […] peuvent être copiées des données dépourvues de lien avec la personne dont le comportement constitue une menace pour la sécurité et l'ordre publics ayant fréquenté le lieu où a été ordonnée la perquisition […][9].

En conséquence, le Conseil constitutionnel déclare inconstitutionnelles les dispositions de l'article 11 relatives à la saisie de données informatiques au motif que

> […] le législateur n'a pas prévu de garanties légales propres à assurer une conciliation équilibrée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et le droit au respect de la vie privée […][10].

Ne subsiste alors plus que la possibilité pour les autorités administratives d'accéder aux données durant le temps de la perquisition[11].

2. Une refonte du régime par la loi n° 2016-987

Si la loi de prorogation suivante, datée du 20 mai 2016[12] ne prévoit plus la possibilité de procéder à des perquisitions, elle est réintégrée avec la loi n° 2016-987 du 21 juillet 2016[13]. La loi remplace l'alinéa 4 de l'article 11, I de la loi n° 55-385 par six nouveaux alinéas venant préciser le régime de la saisie et l'exploitation de données informatiques. Les autorités administratives ont de nouveau la possibilité de copier des données présentant un lien avec une menace à la sécurité ou à l'ordre publics, mais également celle de saisir les supports sur lesquels se trouvent ces données dans le cas où la copie ne pourrait être achevée durant le temps de la perquisition[14]. Réalisée en présence d'un officier de police judiciaire, la copie ne peut être effectuée sans que soit dressé un procès-verbal indiquant les motifs de la saisie et l'inventaire des données saisies[15].

L'un des apports les plus importants de la loi n° 2016-987 est le rôle accordé au juge des référés. Ce dernier doit être saisi par les autorités administratives pour obtenir l'autorisation de procéder, non pas à la saisie, puisque celle-ci a déjà eu lieu, mais à l'exploitation des données[16]. Nul ne peut y avoir accès sans cette autorisation[17]. De plus, le juge exclut de l'autorisation les éléments dépourvus de lien avec la menace[18]. En cas de refus du juge des référés, les autorités administratives doivent détruire les données saisies et / ou restituer les supports saisis dans le cadre de la perquisition[19]. En tout état de cause, les supports doivent être restitués dès que les autorités ont procédé à la copie des éléments en lien avec la menace[20].

Dans un deuxième temps, la loi fixe un délai de conservation des données saisies. L'article 11, I, al. 8 prévoit que les données, autres que celles caractérisant une menace, doivent être détruites dans un délai maximal de trois mois à compter de la date de perquisition ou de la date à laquelle le juge des référés a autorisé l'exploitation[21].

Ce nouveau régime, qui prévoit un encadrement plus strict de la saisie de données, a été globalement validé par

3. Loi n° 55-385 du 3 avril 1955 modifiée par l'article 4 de la loi n° 2015-1501 du 20 novembre 2015, art. 11, I, al. 1.
4. *Ibid.*, art. 11, I, al. 3.
5. *Ibid.*
6. CC, déc. n° 2016-536 QPC du 19 février 2016, *Ligue des droits de l'homme [Perquisitions et saisies administratives dans le cadre de l'état d'urgence]*.
7. O. Le Bot, « Perquisitions administratives : le régime des saisies de données globalement conforme à la Constitution », *Constitutions*, 2017, p. 121.
8. CC., déc. n° 2016-536 QPC, § 14.
9. *Ibid.*
10. *Ibid.*
11. O. Le Bot, « Perquisitions administratives… », p. 121.
12. Loi n° 2016-629 du 20 mai 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence, *Journal officiel de la République française*, n° 117, 21 mai 2016, texte n° 1.
13. Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste, *Journal officiel de la République française*, n° 169, 22 juillet 2016, texte n° 2.
14. Loi n° 55-385 modifié par la loi n° 2016-987 du 21 juillet 2016, art. 11, I, al. 5.
15. *Ibid.*
16. *Ibid.*, art. 11, I, al. 6.
17. *Ibid.*
18. *Ibid.*, art. 11, I, al. 7.
19. *Ibid.*
20. *Ibid.*, art. 11, I, al. 8.
21. *Ibid.*

le Conseil constitutionnel[22]. Ce dernier considère en effet que le nouveau dispositif, « [e]n prévoyant ces différentes garanties légales »[23], permet une « conciliation qui n'est pas manifestement déséquilibrée entre le droit au respect de la vie privée et l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public »[24]. Il a cependant censuré une partie de l'article 11, I, al. 8. En effet, le délai de trois mois susmentionné ne concerne que les données ne caractérisant pas une menace, la loi restant muette au sujet des données caractérisant une menace mais n'ayant pas conduit à la constatation d'une infraction pénale. Or, le Conseil constitutionnel reprend une jurisprudence antérieure en la matière, insistant pour que des délais de conservation, au-delà desquels les données récoltées au moyen d'une technique de recueil de renseignement devaient être détruites, soient institués, afin de répondre aux exigences du droit au respect de la vie privée[25].

3. Un dispositif intégré dans le droit commun

Avec l'entrée en vigueur de la loi du 30 octobre 2017[26], le droit commun intègre désormais les quatre pouvoirs de police essentiels de l'état d'urgence. Le régime des visites et saisies, codifié aux articles L. 229 et suivants du Code de la sécurité intérieure, s'inspire très largement du régime des perquisitions administratives. En conséquence, les mesures concernant la saisie et l'exploitation de données informatiques sont également reprises, à l'article L. 229-5 du même Code, et pratiquement à l'identique des dispositions de l'article 11, I de la loi nº 55-385 dans leur rédaction issue de la loi nº 2016-987, prévoyant des conditions d'application et des garanties similaires. Cependant, à la différence de la législation exceptionnelle de l'état d'urgence, le dispositif de l'article L. 229-5 s'applique à la condition plus stricte que

> […] la visite révèle l'existence de documents, objets ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée[27].

En outre, cette menace doit être en lien avec le risque de commission d'acte de terrorisme[28]. Enfin, la demande d'autorisation d'exploitation est à adresser au juge des libertés et de la détention (JLD) du tribunal de grande instance (TGI) de Paris, et non plus au juge des référés du tribunal administratif[29]. Ce choix se révèle salutaire. Il était en effet surprenant de faire participer le juge administratif au processus de décision, décision sur laquelle il aurait potentiellement pu, par la suite, être amené à statuer. Le nouveau régime suppose également que les visites et la saisie de données soient préalablement autorisées par le JLD[30], là où l'ancien prévoyait que seule l'exploitation des données saisies devait être autorisée, et non la saisie elle-même.

Peu de temps après son entrée en vigueur, le Conseil constitutionnel a eu à se prononcer sur la conformité de cette loi à la Constitution à l'occasion d'une QPC[31]. Par le biais d'un argumentaire se situant dans le prolongement de celui employé dans le cadre de sa décision nº 2016-600 QPC, le Conseil constitutionnel considère que le régime de la saisie de données informatiques est conforme à la Constitution, en ce que ce pouvoir ne peut être employé qu'à des conditions strictes et qu'il est entouré de garanties suffisantes[32].

Il est intéressant de préciser que la saisie de documents et d'objets, en revanche, avait été déclarée contraire à la Constitution dans cette même décision[33] au motif que le législateur n'avait « fixé aucune règle encadrant l'exploitation, la conservation et la restitution des documents et objets saisis au cours de la visite »[34]. Or, la saisie de documents a été réintégrée aux dispositions du Code de la sécurité intérieure relative à la saisie par la loi nº 2019-222 de programmation 2018-2022 et de réforme pour la justice[35], en l'assimilant exactement au régime de la saisie de données, que l'on sait conforme à la Constitution depuis la décision nº 2017-695 QPC.

Innovation récente apparue lors de circonstances exceptionnelles, le régime de la saisie et de l'exploitation de données a rapidement rejoint la palette des pouvoirs de police administrative attribués aux autorités dans le cadre de la lutte contre le terrorisme. Toutefois l'ensemble des garanties procédurales et sa relative proximité avec le régime des perquisitions judiciaires semblent aller dans le sens d'un régime équilibré.

22. CC., déc. nº 2016-600 QPC du 2 décembre 2016, *M. Raïme A. [Perquisitions administratives dans le cadre de l'état d'urgence III]*.
23. *Ibid.*, § 13.
24. *Ibid.*
25. CC, déc. nº 2015-713 DC du 23 juillet 2015, *Loi relative au renseignement*, § 38, 39 et 78.
26. Loi nº 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, *Journal officiel de la République française*, nº 255, 31 octobre 2017, texte nº 1.
27. Code de la sécurité intérieure, art. L. 229-5, I.
28. *Ibid.*
29. Code de la sécurité intérieure, art. L. 229-5, II.
30. *Ibid.*, art. L. 229-1, al. 1.
31. CC, déc. nº 2017-695 QPC du 29 mars 2018, *M. Rouchdi B. et autre [Mesures administratives de lutte contre le terrorisme]*.
32. *Ibid.*, § 64 et 66.
33. *Ibid.*, § 68.
34. *Ibid.*
35. Loi nº 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, *Journal officiel de la République française*, nº 71, 24 mars 2019, texte nº 2, art. 66.

B. Constitutionnalité de la pénalisation du refus de remettre aux autorités judiciaire la clé de déchiffrement d'un moyen de cryptologie

> Protéger les données personnelles dans l'univers numérique, à l'aide notamment du chiffrement, c'est aussi protéger un droit fondamental et, au-delà, l'exercice des libertés individuelles dans cet univers[36].

Indispensable pour assurer la confidentialité des échanges, le chiffrement constitue un moyen de cryptologie qui permet de rendre inintelligibles des données à des tiers à l'aide d'algorithmes[37]. Libre d'utilisation[38], ce procédé, qui englobe tant des logiciels particulièrement sophistiqués que le simple code de verrouillage d'un smartphone, est mobilisé dans de nombreux domaines.

Comme tout moyen de communication, ces données cryptées peuvent être utilisées pour préparer ou commettre des infractions. Aussi leur accès peut-il s'avérer nécessaire pour mener à bien l'enquête de police. Ainsi, la pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie est conforme à la Constitution. C'est là l'apport de la décision nº 2018-696 QPC rendue par le Conseil le 30 mars 2018. Constitue ainsi une infraction spécifique,

> […] le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre […][39].

L'élément matériel de cette infraction spécifique réside donc dans le refus opposé aux autorités de leur remettre, ou de mettre en œuvre, la clé permettant de déchiffrer les données cryptées.

Cette pénalisation du refus de déchiffrement soulève d'importants questionnements tant vis-à-vis des droits de la personne suspectée d'avoir commis l'infraction (1) que de la vie privée et du secret des correspondances des individus en général (2).

1. La pénalisation du refus de remettre la clé de déchiffrement face au droit de ne pas s'auto-accuser

Quand la remise de la convention secrète de déchiffrement est requise à l'égard du suspect lui-même, une question spécifique doit être posée : celle du droit de ne pas s'auto-accuser. Peut en effet être exigé de la part d'une personne qu'elle remette la clé qui permettra d'accéder aux éléments nécessaires pour faire progresser l'enquête dans laquelle elle fait figure de suspect… ! C'est dans cette situation que se trouvait le requérant à l'origine de la QPC[40]. Placé en garde à vue, M. Malek B. avait refusé de communiquer les codes de déverrouillage de ses téléphones[41].

Le droit de se taire[42] ne figurant expressément ni dans la Constitution de 1958 ni dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales[43], le Conseil constitutionnel, comme la Cour européenne des droits de l'homme, sont venus pallier cette lacune. Le Conseil considère ainsi qu'il découle de la présomption d'innocence[44] que « nul n'est tenu de s'accuser »[45]. La Cour européenne des droits de l'homme, quant à elle, déduit de l'article 6[46] relatif au procès équitable le droit pour tout accusé[47] de se taire et de ne point contribuer à sa propre incrimination[48]. À l'instar de la question posée en matière de prélèvements biologiques quelques années auparavant[49], le droit de ne pas s'auto-accuser va-t-il pouvoir se saisir de la question des données numériques cryptées ? À vrai dire, la nouveauté réside uniquement dans la question du numérique. Le Conseil avait déjà affirmé que la pénalisation du refus de la remise de certains documents à des agents de douanes[50] ou de l'autorité de la concurrence et du ministère de

36. Commission nationale de l'informatique et des libertés, « Les enjeux de 2016 (3) : quelle position de la CNIL en matière de chiffrement », 8 avril 2016, en ligne : https://www.cnil.fr/fr/les-enjeux-de-2016-3-quelle-position-de-la-cnil-en-matiere-de-chiffrement.
37. Commentaire de la décision nº 2018-696 QPC du 30 mars 2018, *Malek B. [Pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie]*, p. 1-2.
38. Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, *Journal officiel de la République française*, nº 143, 22 juin 2004, p. 11168, texte nº 2, art. 30, I.
39. Code pénal, art. 434-15-2, al. 1, codifié par la loi nº 92-686 du 22 juillet 1992 portant réforme des dispositions du Code pénal relatives à la répression des crimes et délits contre la nation, l'État et la paix publique, *Journal officiel de la République française*, nº 169, 23 juillet 1992, p. 9857, modifié par la loi nº 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, *Journal officiel de la République française*, nº 129, 4 juin 2016, texte nº 1, art. 16.
40. CC, déc. nº 2018-696 QPC.
41. Commentaire de la décision nº 2018-696 QPC, p. 7.
42. CC, déc. nº 2016-594 QPC du 4 novembre 2016, *M^me^ Sylvie T. [Absence de nullité en cas d'audition réalisée sous serment au cours d'une garde à vue]*, § 3 et Cour EDH, 25 février 1993, *Funke c. France*, nº 10828/84, § 44.
43. Convention EDH, signée à Rome le 4 novembre 1950.
44. Déclaration des droits de l'homme et du citoyen (DDHC) du 26 août 1789, art. 9.
45. CC, déc. nº 2004-492 DC du 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, § 110.
46. Convention EDH, art. 6.
47. Au sens autonome du terme ; en ce sens, voir Cour EDH, 25 février 1993, *Funke c. France*, § 44.
48. *Ibid.*
49. CC, déc. nº 2010-25 QPC du 16 septembre 2010, *M. Jean-Victor C. [Fichier empreintes génétiques]*, § 17.
50. CC, déc. nº 2011-214 QPC du 27 janvier 2012, *Société COVED SA [Droit de communication de l'administration des douanes]*, § 7.

l'Économie[51] ne méconnaissait pas le droit de ne pas s'accuser[52]. La même appréciation est retenue par la Cour européenne des droits de l'homme pour qui une disposition sanctionnant le silence gardé sur l'identité de la personne conduisant le véhicule au moment de l'infraction ne porte pas atteinte « à la substance même du droit des requérants de garder le silence et de ne pas contribuer à leur propre incrimination »[53]. Le Conseil s'est donc, en mars 2018, pleinement inscrit dans sa lignée jurisprudentielle. Reprenant un raisonnement classique[54], il considère que, puisque les dispositions

> […] n'ont pas pour objet d'obtenir des aveux de sa part et n'emportent ni reconnaissance ni présomption de culpabilité mais permettent seulement le déchiffrement des données cryptées[55]

elles ne portent pas atteinte au droit de ne pas s'auto-accuser[56].

La constance jurisprudentielle ne dispense pas de recevoir de légères critiques. L'existence d'une infraction ne contraint-elle pas tout de même à fournir un élément de preuve matériel de sa propre culpabilité ? Il n'est pas question de nier le caractère éminemment nécessaire d'une telle disposition pour la résolution des enquêtes pénales. Mais il n'en demeure pas moins qu'elle emporte des conséquences sur l'effectivité du droit de ne pas s'auto-accuser, fût-ce pour poursuivre

> […] les objectifs de valeur constitutionnelle de prévention des infractions et de recherche des auteurs d'infractions, tous deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle[57].

2. L'insuffisance des réserves émises par le Conseil constitutionnel

Une telle solution ne doit pas pour autant permettre aux autorités de porter une atteinte excessive au droit à la vie privée et à la confidentialité des échanges de l'individu suspecté. Si la communication de la clé de déchiffrement n'est pas incompatible avec le droit de ne pas s'auto-accuser, il est nécessaire que son utilisation soit circonscrite à la seule recherche d'éléments inhérents à l'enquête. La préservation du secret de la vie privée et de la confidentialité des échanges[58] impose aux autorités de ne pas dépasser le cadre de l'enquête.

C'est en ce sens que le Conseil constitutionnel a subordonné l'application de l'article 434-15-2 du Code pénal à la réunion de deux conditions. Dans un premier temps, les autorités doivent établir que la personne suspectée d'avoir commis une infraction doit avoir effectivement connaissance de la clé[59]. Dans un second temps, l'enquête ou l'instruction doivent avoir permis d'identifier au préalable l'existence des données cryptées[60]. Ainsi, les dispositions de l'article 434-15-2 du Code pénal ne permettent pas aux autorités de demander une clé ou une convention secrète de déchiffrement pour, ensuite, vérifier si le support contient des informations liées à l'enquête. Ce dernier fait doit être établi au préalable.

Cependant, ces réserves ne permettent pas de garantir le droit au respect à la vie privée et le secret des correspondances. L'absence de motivation réelle de la part du Conseil constitutionnel à ce sujet est critiquable. Dans ses observations sur l'affaire, le Premier ministre relève notamment qu'il n'est pas exclu qu'une atteinte au droit à la vie privée et au secret des correspondances se réalise dès lors que la communication de la clé de chiffrement par la personne mise en cause permet aux autorités d'accéder au contenu de conversations à caractère privé[61]. Le cas échéant, le Premier ministre atteste que l'atteinte au droit au secret des correspondances est avérée[62]. Il semblerait que le Conseil constitutionnel lui-même ait jugé en ce sens dans un précédent cas concernant les procédures de réquisitions administratives des données de connexion, en estimant que ces dernières, « excluant l'accès au contenu des correspondances »[63], elles ne sauraient « méconnaître le droit au secret des correspondances »[64]. Si l'on raisonne *a contrario*, il semblerait donc qu'une procédure judiciaire permettant l'accès au contenu des correspondances soit contraire au droit au secret des correspondances. Le Conseil constitutionnel, en jugeant que les dispositions de l'article 434-15-2 du Code pénal ne portent pas atteinte au droit de ne pas s'accuser ni au droit au respect de la vie privée et au secret des correspondances[65], s'écarte pourtant de cette conception, fragilisant par la même occasion l'ensemble de ces droits déjà fortement menacés à l'ère du numérique.

51. CC, déc. nº 2016-552 QPC du 8 juillet 2016, *Société Brenntag [Droit de communication de documents des agents des services d'instruction de l'Autorité de la concurrence et des fonctionnaires habilités par le ministre chargé de l'économie]*, § 11 et 12.
52. Commentaire de la décision nº 2018-696 QPC, p. 10.
53. Cour EDH, GC, 29 juin 2007, *O'Halloran et Francis c. Royaume-Uni*, nº 15809/02, § 62.
54. Voir, en ce sens, CC, déc. nº 2016-552 QPC, § 12.
55. CC, déc. nº 2018-696 QPC, § 8.
56. *Ibid*., § 9.
57. *Ibid*., § 7.
58. Droits dégagés par le Conseil constitutionnel des dispositions de l'article 2 de la DDHC ; voir le commentaire de la décision nº 2018-696 QPC, p. 11.
59. CC, déc. nº 2018-696 QPC, § 8.
60. *Ibid.*
61. M. Lacaze, « Constitutionnalité du refus de remise d'une convention secrète de chiffrement – Conseil constitutionnel 30 mars 2018 », *L'actualité juridique. Droit pénal*, 2018, p. 258, note 1.
62. *Ibid.*
63. CC, déc. nº 2015-478 QPC du 24 juillet 2015, *Association French Data Network et autres [Accès administratif aux données de connexion]*, § 17.
64. *Ibid.*
65. CC, déc. nº 2018-696 QPC, § 9.

C. Constitutionnalité sous réserve de la loi relative à la lutte contre la manipulation de l'information : conciliation du principe de sincérité du scrutin avec les libertés constitutionnelles dans leur exercice numérique

La loi nº 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information[66] vise un double objectif. Le premier est d'assurer la transparence des sources et rémunérations liées aux contenus d'information et limiter l'influence d'États étrangers sur les débats électoraux nationaux. Le second est de permettre de suspendre la diffusion de certaines fausses informations, ce qui lui vaut l'appellation de loi *fake news*. La loi organique du 22 décembre 2018 étend l'effet de la loi ordinaire à l'élection présidentielle[67]. Les difficultés causées par un encadrement de la liberté d'expression en période de campagne électorale ont occasionné de profonds désaccords politiques. En premier lieu, le Sénat a rejeté les deux propositions de loi : le 26 juillet 2018, puis le 6 novembre 2018 après l'échec de la commission mixte paritaire. Les sénateurs estimaient que les dispositions existantes, notamment la loi du 29 juillet 1881[68], suffisaient à limiter les abus dans l'exercice de la liberté d'expression[69]. Les deux textes ont finalement été adoptés en lecture définitive par l'Assemblée nationale le 20 novembre 2018. La loi ordinaire a fait l'objet de trois saisines parlementaires du Conseil constitutionnel. Les auteurs contestaient la conformité de ses articles 1, 4, 5, 6, 8, 10 et 11. La loi est ressortie de son passage rue de Montpensier avec une déclaration de conformité à la Constitution nuancée par deux réserves d'interprétation. La conformité de la loi organique à la Constitution dépend par renvoi de celle de la loi ordinaire, c'est donc sur cette dernière que se porte l'examen le plus attentif du Conseil constitutionnel. Cette décision a été l'occasion de rattacher expressément le principe de sincérité du scrutin à l'article 3 de la Constitution[70] et de l'utiliser dans le cadre d'une conciliation avec les autres droits et libertés constitutionnellement garantis. Cette conciliation s'effectue difficilement avec la liberté d'expression s'agissant de la nouvelle procédure de référé (1). Mais elle se fait également avec la liberté d'entreprendre dans le cadre de nouvelles obligations concernant les plateformes numériques (2).

1. La difficile conciliation entre la liberté d'expression et le principe de sincérité du scrutin dans le cadre du nouveau référé

L'article 1er de la loi du 22 décembre 2018 a inséré un article L. 163-2 dans le Code électoral. Ce dernier introduit une procédure de référé visant à prescrire aux hébergeurs de contenus en ligne, ou à défaut au fournisseur d'accès à Internet[71], d'adopter toutes mesures proportionnées et nécessaires pour faire cesser la diffusion de fausses informations relatives aux scrutins électoraux. Cette nouvelle procédure est largement ouverte puisqu'elle peut être initiée par le Ministère public, tout candidat, tout parti ou groupement politique ou toute personne ayant intérêt à agir. Toutefois, celle-ci est limitée dans le temps aux trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises. Le juge des référés ainsi saisi se prononce dans les quarante-huit heures. Les auteurs de la saisine reprochaient au nouvel article de porter une atteinte disproportionnée à la liberté d'expression. Ils s'appuyaient notamment sur l'importance particulière que revêt cette liberté pour le débat politique et les campagnes électorales. Ils soulignaient également l'imprécision des critères retenus par le législateur et le risque que ceux-ci couvrent des propos parodiques ou simplement trompeurs ou erronés, sans pour autant constituer de fausses informations[72].

Après avoir rappelé que la liberté d'expression et de communication se fonde sur l'article 11 de la DDHC[73], le Conseil constitutionnel souligne l'importance de cette liberté, condition de la démocratie et garantie du respect des autres droits et libertés. Cette place particulière de la liberté d'expression, désormais établie[74], n'est évidemment pas sans rappeler la position de la Cour européenne des droits de l'homme[75]. Le Conseil prend également soin de préciser de nouveau[76] que la place singulière de la liberté d'expression concerne également son exercice en ligne au regard de l'importance particulière de ces nouveaux moyens de communication pour la vie démocratique[77]. Il en conclut que les atteintes à cette liberté doivent être nécessaires, adaptées et proportionnées. En l'espèce, il

66. Loi nº 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, *Journal officiel de la République française*, nº 297, 23 décembre 2018, texte nº 2.
67. Loi organique nº 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, *Journal officiel de la République française*, nº 297, 23 décembre 2018, texte nº 1.
68. Loi du 29 juillet 1881 sur la liberté de la presse.
69. CC, déc. nº 2018-773 DC du 20 décembre 2018, *Loi relative à la lutte contre la manipulation de l'information*, § 11.
70. *Ibid.*, § 16.
71. Les opérateurs concernés sont définis par la loi nº 2004-575.
72. CC, déc. nº 2018-773 DC, § 11.
73. *Ibid.*, § 14.
74. CC, déc. nº 84-181 DC du 11 octobre 1984, *Loi visant à limiter la concentration et à assurer la transparence financière et le pluralisme des entreprises de presse*.
75. Cour EDH, 7 décembre 1976, *Handyside c. Royaume-Uni*, nº 5493/72.
76. CC, déc. nº 2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur Internet*.
77. CC, déc. nº 2018-773 DC, § 15.

relève que la liberté d'expression doit être conciliée avec le principe de sincérité du scrutin. Ce dernier est pour la première fois rattaché expressément à l'article 3 de la Constitution. Sans être inexistant, ce rattachement était jusqu'alors implicite[78].

Le Conseil examine ensuite le cadre normatif du référé pour lequel la loi a prévu trois limites. La première est temporelle : l'usage de la nouvelle procédure est restreint à la période des trois mois précédant l'élection. Cet encadrement met en rapport le dispositif et le but recherché par la loi, c'est-à-dire assurer la clarté du débat électoral et la sincérité du scrutin[79]. De plus, le Conseil relève que la procédure est limitée dans son champ d'application car elle concerne uniquement les contenus publiés sur des services de communication au public en ligne qui se prêtent plus aisément à la diffusion massive de fausses informations. Ce faisant, il semble estimer que l'exercice de la liberté d'expression en ligne présente des particularités justifiant une plus grande limitation, ce qui relativise sa position sur l'inclusion des nouveaux moyens de communication dans la liberté d'expression.

Enfin, le Conseil constitutionnel examine la limite matérielle du référé, c'est-à-dire la définition des contenus susceptibles d'initier la procédure. Celle-ci comporte deux éléments dont le premier présente de sérieuses difficultés. Tel que la loi le définit, il s'agit « des allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir »[80]. Pour rejeter l'argument des requérants selon lequel cette formulation couvrirait les opinions et parodies, les « sages » précisent la définition législative des fausses informations comme « celles dont il est possible de démontrer la fausseté de manière objective »[81]. Toutefois, cette seule précision ne permet probablement pas d'exclure les contenus parodiques dont il n'est pas impossible de démontrer la fausseté de manière objective. Il faudrait donc comprendre non pas une mais deux précisions apportées par le Conseil : non seulement la fausseté du contenu doit pouvoir être démontrée de manière objective, mais en plus il ne peut s'agir d'opinions, de contenus parodiques, d'inexactitudes partielles ou de simples exagérations. L'ampleur d'une telle interprétation de la loi justifierait à elle seule une réserve d'interprétation. Toutefois, ce n'est qu'en confrontant le texte ainsi réinterprété à l'importance particulière de la liberté d'expression lors du débat électoral[82] que le Conseil utilise une réserve pour restreindre la définition des fausses nouvelles aux contenus dont les caractères inexact et trompeur et le risque d'altération du scrutin sont manifestes[83]. En effet, le Conseil semble estimer que certaines fausses informations doivent pouvoir être exprimées pour être confrontées à d'autres points de vue critiques. La liberté d'expression produirait « les anticorps aux abus auxquels elle peut donner lieu » et la censure présenterait le risque « que le remède soit pire que le mal »[84]. Moins problématique, le second élément de définition apporté par la loi restreint les fausses informations à celles dont la diffusion est artificielle ou automatisée, massive et délibérée. Le Conseil souligne le caractère cumulatif de ces trois conditions qui sont bien en rapport avec l'objectif de la loi, particulièrement s'agissant de la circulation d'informations en ligne.

C'est ainsi en apportant une réserve d'interprétation conséquente que le Conseil constitutionnel peut considérer l'ajout de l'article L. 163-2 comme étant nécessaire, adapté et proportionné à l'objectif de clarté du débat électoral et de sincérité du scrutin. Il rejette dans le même temps les arguments des parlementaires fondés sur l'incompétence négative de la loi et la méconnaissance des droits de la défense, le droit à un procès équitable, l'objectif de valeur constitutionnelle de bonne administration de la justice et la garantie des droits.

2. La conciliation entre les libertés constitutionnelles et le principe de sincérité du scrutin dans le cadre des nouvelles obligations à destination des plateformes numériques

La loi du 22 décembre 2018 impose aux plateformes numériques une obligation de transparence des financements ainsi qu'une obligation de mise en œuvre de mécanismes de signalement des fausses informations qui doivent faire l'objet d'une publicité.

Dans un premier temps, l'article 1er de la loi introduit une nouvelle infraction à l'article L. 163-1 du Code électoral dont la peine prévue par le nouvel article L. 112 du même Code est d'un an d'emprisonnement et 75 000 € d'amende. L'incrimination vise les opérateurs de plateformes en ligne[85] dont l'activité dépasse un seuil déterminé de nombre de connexions sur le territoire français. La définition de plateforme est comprise de manière assez étendue, couvrant aussi bien les moteurs de recherche, les sites de référencement, les places de marchés, que les réseaux sociaux[86]. Durant les trois mois précédant le premier jour d'élections et jusqu'à la date du tour de scrutin où celles-ci sont acquises, elles sont assujetties à une obligation de transparence sur l'identité des personnes leur versant une rémunération en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général. Elles doivent également publier le montant de

78. CC, déc. nº 2013-673 DC du 18 juillet 2013, *Loi relative à la représentation des Français établis hors de France*, § 6.
79. CC, déc. nº 2018-773 DC, § 19.
80. Loi nº 2018-1202, art. 1er.
81. CC, déc. nº 2018-773 DC, § 21.
82. *Ibid*., § 22.
83. *Ibid*., § 23.
84. Commentaire de la décision nº 2018-773 DC, p. 17.
85. Ces opérateurs sont définis par l'article L. 111-7 du Code de la consommation.
86. Commentaire de la décision nº 2018-773 DC, p. 2.

ces rémunérations lorsque celui-ci dépasse un certain seuil fixé par décret à cent euros hors taxe, pour chaque contenu d'information se rattachant à un débat d'intérêt général[87]. Enfin, les plateformes en ligne ont une obligation de transparence sur l'utilisation des données personnelles dans le cadre de la promotion d'un contenu d'information se rattachant à un débat d'intérêt général. Les auteurs de la saisine soutenaient que les dispositions précitées portaient une atteinte au principe de légalité en raison de l'imprécision de la notion de « contenus d'information se rattachant à un débat d'intérêt général »[88]. Toutefois, en rattachant cette expression au principe de sincérité du scrutin, le Conseil définit ces contenus d'information comme « ceux qui présentent un lien avec la campagne électorale »[89] afin d'écarter le grief tiré de la méconnaissance du principe de légalité. Il est étonnant que le Conseil n'ait pas formulé cette précision sous la forme d'une réserve d'interprétation de manière à lui donner plus de visibilité dans le dispositif. Peut-être ne souhaitait-il pas recourir excessivement à cette technique dans le cadre de cette décision. Les parlementaires soulevaient également une atteinte à la liberté d'entreprendre sur le fondement de l'article 4 de la DDHC[90]. Se fondant sur la précision qu'il a précédemment apportée à la définition des contenus concernés ainsi qu'à la limite temporelle des nouvelles obligations[91], le Conseil en déduit que l'atteinte portée à la liberté d'entreprendre n'est pas disproportionnée[92] eu égard à l'objectif d'intérêt général de clarté du débat électoral qui semble être rattaché au principe de sincérité du scrutin.

Dans un second temps, l'article 11 de la loi impose aux opérateurs de plateformes en ligne de mettre en place un dispositif permettant à leurs usagers de signaler de fausses informations. Ils doivent également mettre en œuvre des mesures complémentaires pouvant porter sur la transparence des algorithmes ou la lutte contre les comptes propageant massivement de fausses informations[93]. Ces dispositions étaient critiquées par les requérants car elles laissent aux opérateurs privés le soin de prendre les mesures pour arrêter la diffusion de fausses informations, notion dont l'imprécision risquerait d'inciter les plateformes à porter une atteinte disproportionnée à la liberté d'expression et de communication[94]. Selon eux, la mesure porterait également une atteinte à la liberté d'entreprendre. Renvoyant à sa propre réserve d'interprétation sur la définition de la notion d'une fausse information[95], le Conseil souligne qu'il appartiendra au juge saisi à l'occasion d'un litige de se prononcer sur les mesures adoptées par les plateformes, et sur leur caractère nécessaire, adapté et proportionné à l'objectif poursuivi. Il en conclut que la loi est proportionnée à l'objectif d'intérêt général de clarté du débat électoral et au principe de sincérité du scrutin. Elle est donc conforme à la Constitution.

Enfin, le Conseil considère qu'une simple obligation de mise en œuvre de mesures dont les modalités sont déterminées par les opérateurs privés, ainsi que la publicité desdites mesures, ne constituent pas, en l'espèce, une atteinte disproportionnée à la liberté d'entreprendre[96]. Il est donc admis que la loi puisse imposer, dans une certaine mesure, une obligation de transparence des algorithmes.

II. Les relations entre les administrés et l'administration

A. Le principe d'*open data* par défaut

Les données ouvertes, ou *open data*, renvoient aux données « qu'un organisme met à la disposition de tous sous forme de fichiers numériques afin de permettre leur réutilisation »[97]. Pour Mélanie Clément-Fontaine, les *open data* visent toutefois

> […] à l'origine, les données publiques, autrement dit, celles qui sont produites par les organismes publics, voire les personnes chargées d'une mission de service public[98].

Ainsi, les données publiques sont les données contenues dans les documents administratifs[99] devant eux-mêmes faire l'objet d'une mise à disposition.

En France, le principe d'accès aux documents administratifs trouve sa source dans la loi du 17 juillet 1978, qui prévoyait la communication de plein droit de ces documents administratifs aux personnes en faisant la demande[100]. Cependant, il était possible d'opposer un

87. Décret nº 2019-297 du 10 avril 2019 relatif aux obligations d'information des opérateurs de plateforme en ligne assurant la promotion de contenus d'information se rattachant à un débat d'intérêt général, *Journal officiel de la République française*, nº 86, 11 avril 2019, texte nº 40.
88. CC, déc. nº 2018-773 DC, § 3.
89. *Ibid.*, § 8.
90. CC, déc. nº 2011-139 QPC du 24 juin 2011, *Association pour le droit à l'initiative économique [Conditions d'exercice de certaines activités artisanales]*, § 3.
91. Commentaire de la décision nº 2018-773 DC, p. 7.
92. CC, déc. nº 2018-773 DC, § 9.
93. Commentaire de la décision nº 2018-773 DC, p. 31.
94. CC, déc. nº 2018-773 DC, § 84.
95. *Ibid.*, § 23.
96. *Ibid.*, § 89.
97. Commission générale de terminologie et de néologie, avis, *Vocabulaire de l'informatique et du droit*, *Journal officiel de la République française*, nº 103, 3 mai 2014, p. 7639, texte nº 107.
98. M. Clément-Fontaine, « La régulation de l'Open data », *LEGICOM*, nº 56, 2016, p. 114.
99. Au sens de l'article L. 300-2 du Code des relations entre le public et l'administration (CRPA).
100. Loi nº 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, *Journal officiel de la République française*, 18 juillet 1978, p. 2851, art. 2.

refus à cette demande, pour diverses raisons aisément compréhensibles, allant de la protection de la vie privée à celle du secret de la défense nationale. Pour surveiller le respect de ces dispositions, était alors créée la Commission d'accès aux documents administratifs (CADA). Le droit d'accès aux documents administratifs allait alors de pair avec le droit à l'information et, par là, renvoyait à la nécessité de transparence de l'action administrative.

C'est sous l'impulsion du droit de l'Union européenne que cette nécessité s'est doublée d'une logique économique. En effet, une directive du 17 novembre 2003[101] a précisé les conditions dans lesquelles les organismes publics ou les organismes chargés d'une mission de service public pouvaient permettre la réutilisation des documents qu'ils diffusaient, c'est-à-dire

> […] l'utilisation par des personnes physiques ou morales de documents détenus par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les documents ont été produits[102].

Toutefois, la directive ne met en place qu'un « ensemble minimal de règles concernant la réutilisation et les moyens pratiques destinés à faciliter la réutilisation de documents existants »[103], sans obliger les États à mettre en place un tel procédé.

Ce fut chose faite avec l'adoption de la directive du 26 juin 2013 modifiant celle de 2003. En effet, l'Union européenne entend dès lors que les États « veillent à ce que les documents [administratifs] puissent être réutilisés à des fins commerciales ou non commerciales »[104] sous des réserves similaires à celles posées par la loi de 1978 (protection de la défense nationale, protection des données à caractère personnel, confidentialité des informations commerciales).

Ces objectifs, économique et commercial d'une part, et de transparence à l'égard des administrés d'autre part, sont d'ailleurs clairement revendiqués au sein des directives de 2003[105] et 2013[106].

C'est cette diffusion des documents administratifs ainsi que leur possibilité de réutilisation qui sont rendues obligatoires en France avec la transposition de la directive de 2013 au sein de la loi pour une République numérique du 7 octobre 2016. En effet, celle-ci prévoit au sein d'une section intitulée « Ouverture de l'accès aux données publiques » que les administrations sont tenues de publier en ligne les documents administratifs ou de les communiquer à toute personne en faisant la demande[107]. Si, à la lecture de l'article 3, la publication pourrait apparaître facultative, il n'en n'est rien puisque l'article 6 précise que l'administration, lorsqu'ils sont disponibles sous forme électronique, « publient en ligne les documents administratifs suivants », parmi lesquels figurent les documents qui doivent être communiqués à toute personne en faisant la demande[108].

De plus, la loi prévoit la possibilité de réutiliser ces informations publiées ou communiquées, « par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus »[109]. La publication des documents administratifs et donc des données publiques qu'ils contiennent à des fins de réutilisation devient donc le principe, ce que traduit la politique d'*open data* par défaut. Toutefois, comme le prévoyait déjà la loi en 1978 ainsi que le droit de l'Union européenne dès 2003, cette publication souffre d'exceptions : les administrations n'ont pas à publier en ligne les documents qui ne sont pas communicables, tels que les avis du Conseil d'État et des juridictions administratives, les documents administratifs relevant de la défense nationale, de la conduite de la politique extérieure de la France, etc.[110]. Elles n'ont pas non plus à publier les documents qui ne sont communicables qu'aux intéressés et qui porteraient atteinte à leur vie privée, au secret médical ou au secret des affaires, ou qui porteraient un jugement de valeur sur une personne physique facilement identifiable, etc.[111]. De la même façon, ne sont pas tenues de publier ces documents, les collectivités territoriales de moins de 3 500 habitants[112], ni les organismes dont le seuil d'agents ou de salariés est inférieur à 50[113].

101. Cette directive a été transposée par l'ordonnance nº 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, *Journal officiel de la République française*, nº 131, 7 juin 2005, p. 10022, texte nº 13. La directive a également été transposée par un décret nº 2005-1755 du 31 décembre 2005 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, pris pour l'application de la loi nº 78-753 du 17 juillet 1978, *Journal officiel de la République française*, nº 304, 31 décembre 2005, p. 20827, texte nº 119.
102. Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *Journal officiel de l'Union européenne*, L 345, 31 décembre 2003, p. 90, art. 2, point 4.
103. *Ibid.*, art. 1er, point 1.
104. Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, *Journal officiel de l'Union européenne*, L 175, 27 juin 2013, p. 1-8, point 3.
105. Directive 2003/98/CE, cons. 5 : « L'amélioration des possibilités de réutilisation des informations émanant du secteur public devrait notamment permettre aux entreprises européennes d'exploiter le potentiel de ces informations et contribuer à la croissance économique et à la création d'emplois ».
106. Directive 2013/37/UE, cons. 3.
107. Loi nº 2016-1321, art. 3, 2°.
108. *Ibid.*, art. 6, II.
109. CRPA, art. L. 321-1 modifié par l'art. 9 de la loi nº 2016-1321.
110. CRPA, art. L. 311-5 modifié par l'ordonnance nº 2016-1360 du 13 octobre 2016 modifiant la partie législative du Code des juridictions financières, *Journal officiel de la République française*, nº 240, 14 octobre 2016, texte nº 2.
111. CRPA, art. L. 311-6 modifié par l'art. 6 de la loi nº 2016-1321.
112. Loi nº 2016-1321, art. 6, II.
113. Décret nº 2016-1922 du 28 décembre 2016 relatif à la publication en ligne des documents administratifs, *Journal officiel de la République française*, nº 303, 30 décembre 2016, texte nº 14, art. 1.

L'application de la politique d'*open data* semble inégale. Ainsi, le tribunal administratif de Paris a estimé que le refus de publier en ligne un rapport, qui avait pourtant été communiqué à une association après avis positif de la CADA, ne peut être ordonné par le juge sans nouvelle saisine de la CADA[114]. Cette décision oblige ainsi les requérants à saisir la CADA une première fois pour qu'elle rende un avis positif sur la communication, puis une deuxième fois pour demander la publication en ligne, dont ils n'ont pas besoin puisqu'ayant déjà le rapport en leur possession. Si le Conseil d'État n'a pas eu l'occasion de se prononcer sur ce phénomène, cette solution montre déjà une certaine réticence à l'égard d'une telle politique.

Cette réserve est également visible dans le domaine singulier des décisions de justice. En effet, si la communication de ces décisions ne pose aucun problème à l'égard des intéressés, il en va autrement lorsqu'elle est demandée par les tiers. Dans ce dernier cas, il n'est pas rare que le greffe refuse de transmettre la décision, à l'instar du président du TGI de Paris dans une ordonnance du 6 octobre 2017. Après le refus de la directrice des services du greffe du TGI de Paris de transmettre les décisions rendues par le tribunal à l'entreprise Doctrine, le président du TGI rejette la requête de Doctrine tendant à enjoindre le greffe à délivrer ces décisions[115]. Toutefois, l'appel formé devant la cour d'appel de Paris est payant pour l'entreprise, puisque l'arrêt enjoint le greffe à publier les décisions[116]. Ce dispositif, logique au regard de la LRN, va pourtant être contredit par une note adoptée le lendemain, qui enjoint l'administration à ne pas diffuser les décisions en masse si cette diffusion répond à des

> […] demandes dont il est manifeste qu'elles ne portent pas sur une ou plusieurs affaires en particulier mais sur la jurisprudence de la juridiction dans une ou plusieurs matières […][117].

La note précise même les motifs du refus, qui pourront se fonder sur « des considérations liées à l'objectif de valeur constitutionnelle de bonne administration de la justice et à la protection des données à caractère personnel »[118].

Faisant écho à cette note, la loi de programmation 2018-2022 et de réforme pour la justice, promulguée le 23 mars 2019, prévoit la mise à disposition en ligne, et à titre gratuit, des décisions de justice, sous réserve d'occultation des noms et prénoms des personnes physiques « mentionnées dans le jugement »[119], ainsi que de toute information permettant de les identifier, si cela portait atteinte à leur vie privée ou à leur sécurité. Si cette réserve s'entend, elle peut également mettre à mal l'application du principe d'*open data* pour les décisions de justice, l'administration pouvant alléguer un manque de moyens matériels ou humains dédiés à l'anonymisation. De la même façon, la loi du 23 mars prévoit que la délivrance des copies des jugements soit faite, « sous réserve des demandes abusives, en particulier par leur nombre ou par leur caractère répétitif ou systématique »[120]. Saisi au titre de l'article 61 de la Constitution, le Conseil constitutionnel n'a pas censuré ces dispositions, estimant qu'elles répondaient à l'objectif de valeur constitutionnelle de bonne administration de la justice[121], malgré leur évidente imprécision. Un tel flou peut dès lors très facilement conduire à des dérives et à une inapplication de l'*open data*, notamment au regard de la réticence marquée des pouvoirs publics à l'égard de ce principe.

B. Action de groupe en réparation des préjudices liés aux données à caractère personnel

La loi relative à la protection des données personnelles en date du 20 juin 2018[122] ouvre aux administrés la possibilité de se grouper afin d'obtenir la réparation des préjudices moraux ou matériels causés par un manquement de même nature[123] aux dispositions du Règlement général relatif à la protection des données personnelles (RGPD)[124] ou de la loi informatique et libertés (LIL)[125]. L'action pourra être dirigée à l'encontre du responsable de traitement de données à caractère personnel, c'est-à-dire la personne

114. TA de Paris, 14 novembre 2018, nº 1800720/5-3.
115. TGI Paris, ch. des requêtes, 6 octobre 2017, nº 17/02017.
116. CA Paris, pôle 2 – ch. 1, 18 décembre 2018, nº 17/22211.
117. Note du ministère de la Justice relative à la communication de décisions judiciaires civiles et pénales aux tiers à l'instance, 19 décembre 2018, point 3.
118. *Ibid.*
119. Loi nº 2019-222, art. 33, II, 1°.
120. *Ibid.*, art. 3, II, 2°.
121. CC, déc. nº 2019-778 DC du 21 mars 2019, *Loi de programmation 2018-2022 et de réforme pour la justice*, § 96. Le Conseil pointe notamment la charge disproportionnée qui pèserait sur l'administration « au regard des moyens dont elle dispose ».
122. Loi nº 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *Journal officiel de la République française*, nº 141, 21 juin 2018, texte nº 1, article 25, 3°.
123. Ancien article 43 ter, devenu article 37 le 1er juin 2019 en application de l'ordonnance nº 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi nº 2018-493 du 20 juin 2018 relative à la protection des données personnelles, et portant modification de la loi nº 78-17 du 6 janvier 1978, *Journal officiel de la République française*, nº 288, 13 décembre 2018, texte nº 5.
124. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *Journal officiel de l'Union européenne*, L 119, 4 mai 2016, p. 1-88.
125. Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *Journal officiel de la République française*, 7 janvier 1978, modifiée.

physique ou morale à qui il revenait de déterminer les finalités et les moyens de ce traitement, ou son sous-traitant[126].

Cette nouvelle voie de recours s'inscrit dans un développement croissant tant des actions collectives (1) que de la protection juridictionnelle des données personnelles (2). Elle revêt par ailleurs un aspect tout particulier devant le juge administratif (3).

1. Une première apparition timide de l'action de groupe en matière de données personnelles limitée à la cessation des manquements

C'est en 2014, par la voie du droit de la consommation, que l'action de groupe a fait son entrée dans notre ordre juridique[127]. Il a toutefois fallu attendre la loi nº 2016-1547 de modernisation de la justice du XXIe siècle, dite J21, pour qu'elle soit ouverte en matière de données personnelles[128]. Elle se limitait alors à la seule cessation des manquements du responsable du traitement ou son sous-traitant devant le juge judiciaire ou administratif – le responsable du traitement prenant dans ce cas la forme d'une « personne morale de droit public ou [d']un organisme de droit privé chargé de la gestion d'un service public »[129]. Toute demande d'indemnisation demeurait ainsi exclue du mécanisme. Il revenait à chacun des administrés lésés d'exercer une action individuelle pour obtenir réparation d'un préjudice personnel pourtant similaire.

Le législateur de 2018 répond ainsi aux critiques formulées lors de l'adoption de la loi J21 qui regrettaient le refus, opposé à ce seul domaine, d'ouvrir l'action en responsabilité. Cela, alors même qu'existait « un certain consensus sur le fait qu'une action de groupe poursuit, en France, la réparation des préjudices liés aux atteintes aux droits individuels »[130]. Cette absence était d'autant plus regrettable que l'absence de menace de dommages-intérêts privait l'action d'une partie importante de sa portée dissuasive. Cette lacune disparaît donc avec la loi du 20 juin 2018[131].

2. L'extension bienvenue du recours collectif à la réparation des violations liées aux données personnelles

La nouvelle action de groupe *réparatrice*[132] s'inscrit dans le mouvement plus large du développement de la protection juridictionnelle des données personnelles qui promeut la « mise en pouvoir d'agir »[133] des individus. Le RGPD fait en effet passer la protection des données personnelles d'une logique de conformité, ou déclarative[134], à une logique de responsabilité[135] de la personne qui collecte et traite les données.

Désormais, les préjudices matériels et moraux, dont les faits générateurs sont postérieurs au 24 mai 2018[136], pourront faire l'objet d'une demande de réparation par la voie de l'action de groupe. Ainsi en est-il d'une collecte illicite ou déloyale[137], de l'absence de consentement de la personne concernée[138] ou encore du recueil de données révélant

> […] la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique […][139].

Qu'elle tende à la seule cessation d'un manquement ou que sa visée soit réparatrice, l'accès à l'action est limité. Elle ne peut être exercée que par les personnes visées par la LIL. Sont concernées, à titre principal, les associations régulièrement déclarées depuis cinq ans au moins et ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel[140]. Il reviendra aux personnes lésées, à l'issue du jugement en responsabilité, de donner mandat de représentation à la personne morale demanderesse[141] pour obtenir indemnisation. Héritée du droit américain, qui n'opère pas de distinction entre ordres juridictionnels, l'action peut être menée tant en matière privée que publique[142].

126. Règlement (UE) 2016/679, art. 4.7.
127. Loi nº 2014-344 du 17 mars 2014 relative à la consommation, *Journal officiel de la République française*, nº 65, 18 mars 2014, texte nº 1, art. 1 et 2.
128. Loi nº 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, *Journal officiel de la République française*, nº 269, 19 novembre 2016, texte nº 1, titre V.
129. Code de justice administrative, art. L. 77-10-3.
130. M.-J. Azar-Baud, « Action de groupe : droits, préjudices et prétention processuelle dans les actions de groupe », *La semaine juridique, entreprise et affaires*, nº 26, 2017, 1357, p. 29.
131. Loi nº 2018-493, art. 25, 3°.
132. Loi nº 78-17, art. 37, III.
133. C. Zolynski, « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un empowerment renforcé », *Dalloz IP/IT*, 2018, p. 470.
134. N. Martial-Braz, « L'abus de textes peut-il nuire à l'efficacité du droit ? », *Dalloz IP/IT*, 2018, p. 459.
135. Voir notamment A. Danis-Fatôme, « Protection des données : quelles actions judiciaires en cas de violation du RGPD ? », *Communication – Commerce électronique*, 2018, étude nº 4, dossier nº 18, p. 1.
136. Loi nº 78-17, art. 37, III, al. 2.
137. *Ibid.*, art. 4.
138. *Ibid.*, art. 5, 1°.
139. *Ibid.*, art. 6, I.
140. *Ibid.*, art. 37, IV.
141. Code de justice administrative, art. L. 77-10-10 et art. 69 de la loi nº 2016-1547.
142. Loi nº 78-17, art. 37, II.

3. Une indemnisation collective ouverte à l'encontre des pouvoirs publics

Les données à caractère personnel doivent bien sûr être protégées des fins commerciales pour lesquelles elles peuvent être collectées et utilisées devant le juge judiciaire[143]. Mais il convient encore de prémunir les citoyens contre les potentielles indiscrétions de l'administration. L'action de groupe à visée réparatrice peut ainsi être exercée à l'encontre des personnes publiques et des personnes privées chargées de services publics, responsables du traitement de données personnelles.

Dans ce cadre, est ouvert au citoyen administratif un recours identique à celui qu'il aurait exercé à l'encontre d'une personne privée dépourvue de toute mission de service public, cela que l'action s'exerce ou non sur un marché concurrentiel. Que les règles concernant le traitement de vos données à caractère personnel aient été violées par Facebook ou l'État français, l'action conserve la même forme, seul varie le juge compétent. Le législateur reconnaît la possibilité pour l'administration, entendue au sens le plus large, d'être auteure de violations massives des données personnelles au même titre qu'une entreprise privée.

L'action de groupe vient ainsi jouer un rôle pour une meilleure démocratie administrative. Elle influe, par son caractère collectif, sur les relations entre le citoyen et l'administration, assurant l'effectivité des dispositions de la LIL et du RGPD. Mais l'intérêt de l'action en matière administrative aurait pu être plus poussé. Seule peut en effet être recherchée la responsabilité… du responsable du traitement (ou de son sous-traitant). Ainsi la Commission nationale de l'informatique et des libertés (CNIL) ne saurait faire l'objet d'une action de groupe alors même qu'une carence dans sa mission de contrôle[144] aurait pu être constatée. Cette autorité administrative est d'ailleurs amenée à participer à la procédure. En effet, elle doit être informée dès lors qu'une action est introduite[145].

Notons que, pour l'heure, aucune action de groupe en matière de données personnelles n'a été introduite devant le juge administratif. Cela alors même que, par ses particularités, elle pouvait sembler plus efficace que sa version judiciaire[146]. Pour autant, l'heure étant aux tendances sécuritaires, la possibilité de faire valoir collectivement le respect des règles en matière de protection des données à caractère personnel apparaît relever d'une nécessité.

C. Action administrative et traitements algorithmiques

1. Les traitements algorithmiques fondant une décision administrative individuelle

Comme nous le rappelions lors de la précédente édition de la chronique des droits numériques[147], le législateur est intervenu dans le but d'apporter une certaine transparence aux décisions administratives individuelles prises sur le fondement de traitements algorithmiques. L'article L. 311-3-1 du Code des relations entre le public et l'administration (CRPA)[148] dispose que les décisions administratives individuelles prises sur le fondement d'un traitement algorithmique doivent comporter une mention explicite qu'un tel traitement est intervenu afin que l'intéressé demande le cas échéant « les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre » au regard de sa situation individuelle[149]. Parallèlement à cette disposition, l'article L. 312-1-3 du même Code précise que les administrations

> […] publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles[150].

Dans ce domaine, la CNIL s'est illustrée par une décision du 30 août 2017[151] en mettant en demeure le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation (MESRI) en raison de l'opacité entourant la plateforme Admission Post-Bac relative à la préinscription des lycéens dans les établissements de l'enseignement supérieur. Cette décision repose notamment sur le fait que ladite plateforme prenait

> […] des décisions produisant des effets juridiques à l'égard des personnes sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé […][152]

et ce sans la moindre intervention humaine. Afin de remédier à cette situation, une nouvelle plateforme a vu le jour par arrêté[153], dénommée Parcoursup. Il s'agit cette fois-ci non pas d'un traitement exclusivement automatisé, effectuant un tirage au sort entre les candidats dès lors que « le nombre de candidats remplissant les mêmes critères

143. En vertu de l'art. 826-2 du Code de procédure civile.
144. Loi nº 78-17, art. 8, 2°.
145. Loi nº 78-17, art. 37, II.
146. M.-J. Azar-Baud, « Variations autour du régime de l'action de groupe », *La semaine juridique, entreprise et affaires*, nº 27, 2017, 1380, p. 42.
147. Q. Butavand, L. Duval, Y. Paquier, « Chronique de jurisprudence des droits numériques 2016-2017 », *Cahiers de la recherche sur les droits fondamentaux*, nº 15, 2017, p. 199.
148. Complété par l'art. R. 311-3-1-2 du CRPA.
149. Pour les exceptions, prévues à l'article L. 311-5 du CRPA, voir *infra*.
150. CRPA, art. L. 312-1-3.
151. CNIL, déc. nº MED-2017-053 du 30 août 2017 mettant en demeure le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation.
152. *Ibid.*
153. Arrêté du 28 mars 2018 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Parcoursup », *Journal officiel de la République française*, nº 74, texte nº 46, 29 mars 2018.

reste supérieur au nombre de places disponibles »[154], mais d'une aide à la prise de décision, faisant donc intervenir des humains dans l'étude des dossiers.

Le MESRI, conformément à l'article L. 612-3, II du Code de l'éducation, a décidé de publier le code source du traitement automatisé de la plateforme nationale ainsi que le cahier des charges synthétiques[155]. Mais les algorithmes, dits *locaux*, utilisés par certaines équipes pédagogiques universitaires chargées de l'examen des candidatures dans les établissements, n'ont pas fait l'objet à ce jour d'une quelconque publicité.

En effet, la loi nº 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants est venue modifier l'article L. 612-3 du Code de l'éducation, précisant qu'

> Afin de garantir la nécessaire protection du secret des délibérations des équipes pédagogiques chargées de l'examen des candidatures présentées dans le cadre de la procédure nationale de préinscription prévue au même deuxième alinéa, les obligations résultant des articles L. 311-3-1 et L. 312-1-3 du code des relations entre le public et l'administration sont réputées satisfaites dès lors que les candidats sont informés de la possibilité d'obtenir, s'ils en font la demande, la communication des informations relatives aux critères et modalités d'examen de leurs candidatures ainsi que des motifs pédagogiques qui justifient la décision prise[156].

Cette disposition a pour conséquence de dénaturer de manière significative l'esprit de la loi pour une République numérique[157] qui avait pourtant vocation à contribuer à une plus grande transparence des décisions administratives individuelles fondées sur un traitement algorithmique. Le Défenseur des droits a été saisi de nombreuses demandes allant dans le sens d'une transparence des algorithmes dits *locaux* utilisés par les universités dans la sélection des candidatures, notamment car ces traitements algorithmiques opaques risquaient d'ouvrir la voie à l'existence de pratiques discriminantes dans l'évaluation des dossiers. Par une décision en date du 18 janvier 2019[158], le Défenseur des droits considère que « le secret des délibérations ne s'oppose pas à l'information des candidats sur le contenu exact et la manière précise d'évaluation des candidatures »[159]. En effet, selon lui, une transparence des critères sur lesquels les dossiers sont examinés ne porte pas atteinte aux principes de souveraineté du jury et du secret des délibérations dans la mesure où la publication de ces informations

> […] ne vise pas à dévoiler le contenu de l'appréciation portée sur chaque candidature, mais uniquement les critères pris en compte dans cette appréciation ainsi que leur méthode d'application[160].

Dans le même temps, le tribunal administratif de Guadeloupe a été saisi par un syndicat étudiant d'une demande de communication des procédés algorithmiques utilisés par l'université des Antilles dans le cadre de la sélection des candidatures Parcoursup. Par un jugement en date du 4 février 2019[161], le tribunal annule la décision implicite de refus de la communication des procédés algorithmiques *locaux* au syndicat et décide d'enjoindre l'université de procéder à ladite communication au motif que cette dernière ne porte pas atteinte au secret des délibérations. En effet, cette communication ne porte que sur la nature des critères pris en compte dans le traitement des candidatures, c'est-à-dire leur pondération ou encore leur hiérarchisation, et aucunement sur « l'appréciation portée par la commission sur les mérites de chacune de ces candidatures »[162]. De plus, pour le juge administratif, puisque la demande n'émane pas d'un candidat, mais d'un tiers, la communication des procédés algorithmiques ainsi que des codes sources de ces programmes est fondée. En effet, le législateur n'a pas écarté dans l'article L. 612-3, I du Code de l'éducation la disposition de l'article L. 311-1 du CRPA qui permet notamment à toute personne qui en fait la demande d'obtenir la communication des documents administratifs qui sont détenus par l'administration[163]. À ce jour, l'université des Antilles entendait se pourvoir en cassation devant le Conseil d'État[164].

2. Les décisions administratives individuelles prises sur le fondement exclusif d'un traitement algorithmique

Lors de son adoption, le RGPD, accompagné d'une directive du même jour[165], a laissé aux États membres des marges de manœuvre substantielles. C'est ce qui a notamment permis au législateur d'autoriser le recours à des décisions administratives individuelles exclusivement

154. CNIL, déc. nº MED-2017-053.
155. Mis en ligne le 21 mai 2018, disponible à cette adresse : http://www.enseignementsup-recherche.gouv.fr/cid130453/parcoursup-publication-du-code-informatique-des-algorithmes.html.
156. Code de l'éducation, art. L. 612-3, I, al. 5.
157. La loi nº 2016-1321 avait introduit les dispositions relatives à la transparence des traitements algorithmiques dans le CRPA.
158. Défenseur des droits, déc. nº 2019-021 du 18 janvier 2019.
159. *Ibid*., § 39.
160. *Ibid*.
161. TA Guadeloupe, 4 février 2019, *UNEF c. université des Antilles*, nº 1801094.
162. *Ibid*., cons. 11.
163. Sauf s'il s'agit de secrets protégés par la loi, voir *supra*.
164. A. Saviana, « Transparence de Parcoursup : une bataille gagnée en Guadeloupe, mais pas la guerre… », *Marianne*, 7 février 2019, en ligne : https://www.marianne.net/societe/transparence-parcoursup-universite-guadeloupe-justice.
165. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *Journal officiel de l'Union européenne*, L 119, 4 mai 2016, p. 89-131.

automatisées, alors qu'elles étaient auparavant interdites. À ce titre, le législateur français a transposé ces dispositions dans le droit national en modifiant la LIL[166]. Alors que la LIL précisait qu'

> Aucune […] décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité[167],

les nouvelles dispositions prévoient désormais des exceptions[168]. Par une décision du 12 juin 2018, le Conseil constitutionnel a notamment été amené à contrôler la conformité de la nouvelle rédaction de l'article 10 avec la Constitution[169].

Les requérants estimaient[170] que l'existence de ces décisions individuelles prises sur le fondement exclusif de traitements algorithmiques équivaudrait à un renoncement du pouvoir d'appréciation de l'administration concernant les situations individuelles, ce qui méconnaîtrait la garantie des droits et l'article 21 de la Constitution. Tel serait particulièrement le cas pour les algorithmes d'apprentissage automatique, qui sont « susceptibles de réviser eux-mêmes les règles »[171] ; ces algorithmes empêcheraient également l'administration de connaître les véritables règles fondant ces décisions administratives. Autre interrogation soulevée par les requérants : en acceptant ce type de décision automatisée, le législateur porterait atteinte « aux principes de valeur constitutionnelle régissant l'exercice du pouvoir réglementaire »[172] puisque, d'une part, l'administration abandonnerait son pouvoir réglementaire à des algorithmes capables de modifier les règles par eux-mêmes, et, d'autre part, le recours à ces algorithmes ne permettrait pas de s'assurer que ces derniers appliquent bel et bien le droit existant. De plus, en ce qui concerne le recours aux algorithmes auto-apprenants, dans la mesure où ils sont susceptibles de réviser les règles qu'ils appliquent eux-mêmes, il en résulterait une imprévisibilité méconnaissant le principe de publicité des règlements. Il ressort du dernier moyen soulevé par les requérants sur ce fondement que les dispositions contestées manqueraient de portée normative, ou, qu'à défaut, « elles seraient contraire, par leur complexité, à l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi »[173].

Pour les sages de la rue de Montpensier, ces dispositions ne sont pas contraires à la Constitution en ce que le législateur a défini

> […] des garanties appropriées pour la sauvegarde des droits et libertés des personnes soumises aux décisions administratives individuelles prises sur le fondement exclusif d'un algorithme[174].

Toutefois, le Conseil vient préciser les conditions du recours par l'administration aux traitements algorithmiques auto-apprenants. Il rappelle que l'adoption de décisions administratives individuelles prises sur le fondement exclusif d'un traitement algorithmique ne peut être effectuée que si les règles et critères sont définis à l'avance par le responsable du traitement. Ces algorithmes n'autorisent pas l'administration à fonder « des décisions sans base légale, ni à appliquer d'autres règles que celles du droit en vigueur »[175]. Il en résulte que le recours à ces algorithmes ne peut être perçu comme une renonciation au pouvoir réglementaire.

Le Conseil rappelle que ces décisions automatisées sont par ailleurs soumises au respect de trois conditions sous peine d'illégalité[176]. Premièrement, elles doivent respecter les obligations précisées par l'article L. 311-3-1 du CRPA. Le Conseil précise toutefois que, dans les hypothèses où les principales caractéristiques de l'algorithme ne peuvent être communiquées pour des raisons de secrets ou d'intérêts énoncés au 2° de l'article L. 311-5 du même Code, « aucune décision ne peut être prise sur le fondement exclusif de cet algorithme »[177]. Il apparaît donc que la transparence de ces algorithmes est pour le Conseil la condition *sine qua non* des décisions prises exclusivement sur le fondement de traitements algorithmiques. Deuxièmement, ces décisions administratives individuelles doivent être susceptibles d'un recours administratif ou contentieux[178]. En cas de tel recours, l'administration doit être susceptible de se prononcer sur la décision « sans pouvoir se fonder exclusivement sur l'algorithme »[179]. Ensuite, si le juge administratif est saisi d'un recours contre cette décision, l'administration doit être en capacité de communiquer à la juridiction les caractéristiques de l'algorithme. Troisièmement, un traitement algorithmique ne peut fonder exclusivement une décision s'il porte sur des données à caractère personnel sensibles[180].

166. Loi nº 2018-493.
167. Loi nº 78-17 modifiée par la loi nº 2004-801 du 6 août 2004, art. 10.
168. Loi nº 2018-493, art. 21.
169. CC, déc. nº 2018-765 DC du 12 juin 2018, *Loi relative à la protection des données personnelles*.
170. *Ibid*., § 66.
171. *Ibid*.
172. *Ibid*.
173. *Ibid*.
174. *Ibid*., § 72.
175. *Ibid*., § 69.
176. *Ibid*., § 70.
177. *Ibid*.
178. Conformément au chapitre 1er titre 1er du livre IV du CRPA.
179. CC, déc. nº 2018-765 DC, § 70.
180. Sont considérées comme des données à caractère personnel sensibles, les catégories de données listées à l'art. 8, I, de la loi nº 78-17.

Enfin, concernant le responsable du traitement, il doit avoir la maîtrise du traitement[181] et ses évolutions, afin d'être en capacité d'expliquer au demandeur, sous une forme intelligible, la façon dont le traitement a été mis en œuvre à son égard. Par ailleurs, en l'absence de contrôle et de validation des algorithmes d'apprentissage automatique par le responsable de traitement, ces algorithmes auto-apprenants, susceptibles de modifier les règles eux-mêmes, ne pourront fonder exclusivement une décision administrative individuelle.

181. CC, déc. nº 2018-765 DC, § 71.